(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 353 292 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
15.10.2003 Bulletin 2003/42

(51) Int Cl.7: G06K 9/20, G07C 9/00

(21) Application number: 02252601.6

(22) Date of filing: 12.04.2002

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE TR
Designated Extension States:
AL LT LV MK RO SI

(71) Applicant: STMicroelectronics Limited
Marlow, Buckinghamshire SL7 1YL (GB)

(72) Inventor: Dennis, Carl
Balerno, Edinburgh EH14 7HS, Scotland (GB)

(74) Representative: Cooper, John et al
Murgitroyd & Company,
Scotland House,
165-169 Scotland Street
Glasgow G5 8PL (GB)

(54) Biometric sensor apparatus and methods

(57) Optical biometric sensor apparatus and methods for analysing images of biometric features such as fingerprints and adapted to distinguish between live body members and inanimate objects, and to detect spoofing devices applied to live body members. Live body members are detected by transmitting IR light from a first IR light source (LED) 14 through an object 10 to an image sensor 20. The IR transmission characteristics of a live body member vary with the human heartbeat, and multiple images are analysed to verify whether the object is a genuine live body member. A visible light source (LED) 18 illuminates the object 10 for obtaining a detailed image from the sensor for conventional biometric analysis. Transmitted IR images and reflected visible light images are also processed in order to detect the presence of spoofing devices applied to live body members. Muliple IR and visible light sources of different wavelengths may be employed for this purpose.

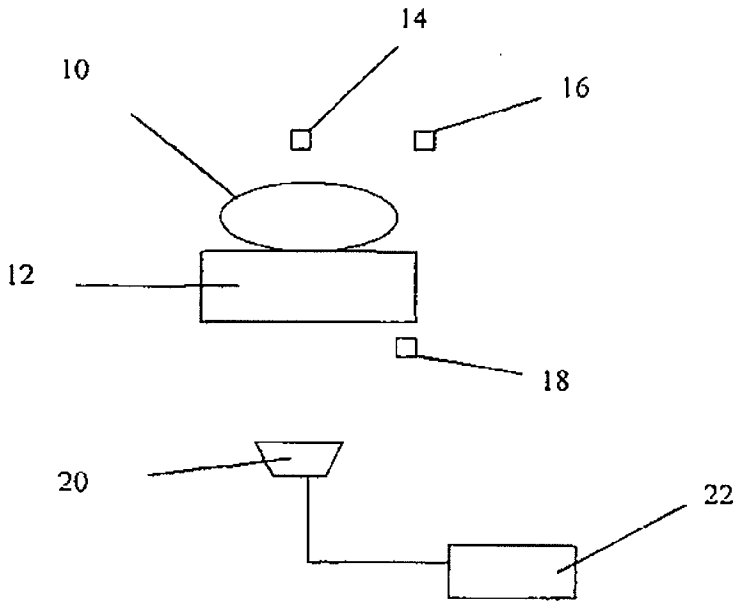

Fig. 1

EP 1 353 292 A1

Description

[0001] The present invention relates to biometric sensor apparatus and methods. More particularly, the invention relates to apparatus and methods using optical imaging of fingerprints, handprints or the like to verify a person's identity, and which are resistant to "spoofing". The invention is particularly concerned with determining whether a finger, hand or the like presented to a biometric imaging device is a live finger, hand etc.

[0002] To be secure, identification systems need to be robust against fraud; i.e. to ensure that one person cannot pass themselves off as another person.

[0003] The field of biometrics relates to the statistical analysis of physiological characteristics. For the purposes of identification for security or other purposes, features such as finger prints or retinal scans can be used to uniquely identify individuals.

[0004] Every person has a unique set of fingerprints, and this provides a basis for identification. An image of a fingerprint can be taken and analysed to see if it matches a recorded sample of the user's fingerprints. This is done by analysing a number of details, or "minutiae" of the fingerprint. The greater the number of minutiae that are analysed, the less are the chances of incorrectly identifying an individual.

[0005] However, a biometric identification system that relies solely on mathematical analysis of simple optical images can be easily spoofed, as a copy of the pattern of a fingerprint can be easily made and presented to a reader device.

[0006] Accordingly, systems have been developed to identify whether the finger to be identified is indeed a three-dimensional finger, rather than just a photocopy or suchlike. Such a system is disclosed in US 6 292 576 (Brownlee). A finger to be identified is placed on a platen and is illuminated by two light sources. The first light source illuminates the finger from directly below the finger, and a positive image is obtained, and the second light source is positioned at an angle greater than the critical angle so that the beam is subject to frustrated total internal reflection (FTIR) to obtain a negative image. The images can then be added, and if a true finger is present, the two images will cancel each other out, whereas if a spoof is present, the images from the two light sources will reinforce each other.

[0007] Such methods using FTIR are well explained in US 6 292 576 and are well known in the art. However, such methods can still be spoofed, for example by rubber models of a finger.

[0008] Therefore, besides analysing the details of a fingerprint, it is desirable for a biometric identification system to verify the presence of a live finger (or other relevant body member).

[0009] International Patent Publication Number WO 01/24700 gives some examples of such techniques. In this case, the ridges of the fingerprint act as one plate of a capacitor. Properties of a live finger such as perspiration, warmth, and pressure, mean that the conductivity of the ridges will change, thus affecting the capacitance. Thus, a finger can be tested with solid state capacitive sensors to see if it has the electrostatic properties that are characteristic of a live finger.

[0010] Such methods and other examples of biometric identification are well known in the art. However, they are expensive to implement.

[0011] There is a need for a live finger detection apparatus that is robust against spoofing and that can be easily manufactured, installed and used.

[0012] The present invention seeks to provide biometric sensor apparatus and methods employing optical imaging of a body member such as a finger, hand or palm, and adapted to identify a live body member.

[0013] As used herein, "optical image sensors" means sensors that are responsive to electromagnetic radiation at least in the visible and infra red (IR) or near-IR spectra. Hereafter, references to IR include near-IR.

[0014] Apparatus and methods in accordance with the present invention are defined in the appended claims.

[0015] The present invention will now be described, by way of example only, with reference to the accompanying drawing, in which:

> Fig. 1 is a block diagram schematically illustrating an embodiment of a biometric sensor apparatus in accordance with the invention.

[0016] The invention will be described in relation to systems for biometric identification based on fingerprints, but is also applicable to identification based on unique characteristics of other body members, particularly hand or palm prints.

[0017] As shown in Fig. 1, a preferred embodiment of a biometric identification system in accordance with the invention is adapted to read and analyse a fingerprint of a fingertip 10 placed in contact with a translucent platen 12. It will be evident to those skilled in the art that in this context the term "translucent" includes the case where the platen 12 is in fact transparent. At least a first and preferably first and second IR illumination sources 14 and 16, suitably light emitting diodes (LEDs), are arranged above the platen 12 to transmit light of selected frequencies in the IR band through the fingertip 10 and platen 12. At least a first visible illumination source 18, again suitably an LED, is arranged below the platen 12 to transmit visible light through the platen 12 for reflection from the fingertip 10 back through the platen 12.

[0018] An optical image sensor 20, suitably a solid state image sensor such as a CCD or, most preferably, a CMOS device, is arranged below the platen 12 to receive transmitted light from the first and second IR LEDs 14 and 16 and reflected light from the visible LED 18. For the purposes of the present invention, the image sensor 20 is suitably a monochromatic (greyscale) sen-

sor, rather than a colour sensor. One or more lenses or the like (not shown) may be provided between the platen 12 and the sensor 20 as required. The sensor 20 is connected to data storage and processing means 22 for storing and processing signals received from the sensor 20.

[0019] As shall be described in more detail below, the first IR LED 14 is used in combination with the sensor 20 for live finger detection in accordance with the invention. The visible LED 18 is used in combination with the sensor 20 for obtaining a detailed image of a fingerprint for biometric identification, in a manner that is well known in the art. In accordance with further aspects of the invention, the first and/or second IR LEDs 14 and 16 are used in combination with the visible LED 18 and sensor 20 to provide additional protection against spoofing; e.g. by a fake fingerprint applied to a live fingertip.

[0020] As noted above, the first IR LED 14 is used in determining whether the fingertip 10 is a live finger, and not a spoofing device such as an imitation finger. For this purpose, the invention employs principles used in the medical field of pulse oximetry. The tissues of a body member such as a fingertip are almost transparent to IR light. However, blood absorbs IR light. This phenomenon is exploited in pulse oximetry for a variety of clinical purposes, including the detection of heart rate, the sinus rhythm of the heart beat, the presence of blood vessels and the percentage of dissolved oxygen in the bloodstream. The present invention applies such techniques in a simplified form for biometric purposes, to detect characteristics of a beating human heart that are present in a live finger but absent in a spoofing device.

[0021] During the pulsatile phase of a heart beat, blood flows through the arteries of a finger, causing them to dilate, while other parts of the finger, such as the tissue and bone, and the venous blood vessels do not change in diameter. Therefore, the intensity of transmitted light will vary between the pulsatile phase and non-pulsatile phase as a result of the blood flow. This difference in intensity of transmitted light can form the basis for forming an image of the blood vessels in a finger and for gathering information about the blood flow in these vessels.

[0022] The intensity will vary according to the Lambert-Beer law, which states that the intensity of a beam of monochromatic radiation varies exponentially with the medium's thickness.

[0023] A pulse oximeter is designed to calculate the respective levels of various types of haemoglobin in the blood, based on the different absorption coefficients of oxygenated and de-oxygenated blood. However, the present invention is not concerned with making such detailed measurements, as it merely needs to detect the presence of a live finger.

[0024] As shown in Fig. 1, a finger 10 to be identified is placed on a transparent platen 12. First IR LED 14 transmits light at a selected IR wavelength. The choice of wavelength is limited by the transmission characteristics of the fingertip and the sensitivity of the sensor 20. The minimum wavelength that is usefully transmitted through a fingertip is about 700 nm. The maximum wavelength detectable by a conventional optical CMOS sensor is about 1100 nm. Conventional, nominally monochromatic LEDs typically have a bandwidth of the order of 20 to 50 nm. In this preferred embodiment, a monochromatic LED having a nominal wavelength of 850 nm is suitable, but LEDs having nominal wavelengths up to 1100 nm may be used. Higher wavelengths could be used with specialised sensors. However, for the purposes of the present invention it is preferable to use a wavelength that is detectable by a conventional image sensor, which is also employed for obtaining the detailed fingerprint image for biometric identification.

[0025] For the purpose of live finger detection, at least two transmitted IR images are required for comparison with one another, in order to detect a pulse. For practical purposes it desirable to capture a larger number of images over a period of time determined by typical human heartrates, so as to obtain sufficient data to verify the existence of a genuine human pulse waveform.

[0026] In the preferred embodiment, the pulse data obtained from the IR images are analysed to make sure that the waveform corresponds to a typical sinus waveform indicative of a human heart beat, and then the period of the heart beat is measured, to see if it falls into a predetermined range of typical human heart beats. To accomplish this, the data must be sampled at an adequate rate, preferably of the order of five to ten times the Nyquist frequency for the highest frequency component of a typical heart beat. Therefore, the sensor 20 might be required to process hundreds or thousands of frames of information per second.

[0027] A typical image sensor 20 for obtaining a detailed fingerprint image for biometric identification may have a pixel array typically comprising anything between 50,000 and 300,000 pixels. However, for the purposes of live finger detection in accordance with the present invention, it is only necessary to capture and process data from a small proportion of these pixels. For example, data may be collected from a window of about sixty-four pixels for each frame. The data value measured for each frame could be the average of the data value for each of the sixty-four pixels. This facilitates the high sampling rate referred to above.

[0028] The live finger detection described thus far protects an optical fingerprint reader against spoofing by inanimate objects or images, in accordance with one aspect of the invention. The visible LED 18 and sensor 20 are used firstly to obtain detailed fingerprint images for biometric identification in a manner that is well known in the art and which will not be described in detail herein. In accordance with a further aspect of the invention, the visible LED 18 is also used in combination with the first and/or second IR LEDs 14 and 16 and the sensor 20 to provide further protection against spoofing by imitation fingerprints applied to live fingertips, as shall now be de-

scribed.

[0029] In accordance with this further aspect of the invention, images obtained by one or more IR light sources in transmission mode (through the fingertip) are compared with images obtained by one or more visible light sources in reflection mode (from the fingertip) to determine whether they are consistent with a genuine finger or whether they indicate the presence of a spoofing device.

[0030] In a similar manner to the above-described embodiment of the invention, data may be collected from a window of about sixty-four pixels for each frame, in order to facilitate the high sampling rate referred to above.

[0031] A frame of data, or several frames averaged in order to reduce noise, is acquired under each illuminant. The human finger transmits and reflects light in well recognised proportions, giving it a particular "colour" defined by the intensity of the measured pixels. A spoofing device that is not itself made of flesh will not have this characteristic colour.

[0032] Where multiple IR light sources are used, it is preferred that these should emit light in non-overlapping IR wavebands, within the limits discussed above for the first IR LED 14. However, partially overlapping IR wavebands may be used, as long as the two signals are distinguishable.

[0033] Similarly, where multiple visible light sources are used, these should emit light in non-overlapping visible wavebands (typically within the range 380-780 nm). However, partially overlapping wavebands could be used as long as they are distinguishable.

[0034] The use of more IR and/or visible light sources provides more data at different wavelengths, improving the reliability of the system. However, it is desirable to minimise the number of light sources in order to minimise the cost and complexity of the system. As a minimum, one IR and one visible light source are required to provide live finger detection and additional anti-spoofing functions together with biometric identification. The addition of a second IR source 16 improves robustness at minimal additional cost. Where the first IR LED has a wavelength of 850 nm, as described above, the second IR LED 16 might suitably have a wavelength of 750 nm.

[0035] In use, the system would preferably perform live finger detection as a first step. If this test is passed, the secondary anti-spoofing test would be performed. Only once both these tests had been passed would the system perform full biometric analysis of the detailed fingerprint image.

[0036] The data storage and processing means 22 may comprise any suitable types of memory and processor, located locally to or remote from the light sources and sensor. If they are located locally, they may be integrated into the same IC as the sensor 20 or be provided on a PCB shared with the sensor.

[0037] Improvements and modifications may be incorporated without departing from the scope of the invention as defined in the appended claims.

Claims

1. Biometric sensor apparatus comprising:

   a translucent platen having a first side against which a body member to be analysed by the apparatus is placed, in use of the apparatus, and a second side;
   at least one IR light source located on the first side of the platen for transmitting light through the body member and the platen to the second side of the platen;
   an optical image sensor located on the second side of the platen for detecting light transmitted through the body member and the platen.

2. The apparatus of claim 1, further including at least one visible light source located on the second side of the platen and arranged such that light from the visible light source is transmitted through the platen and reflected by the body member for detection by the image sensor.

3. The apparatus of claim 1 or claim 2, further including data storage and processing means for storing and processing signals output from the image sensor.

4. The apparatus of claim 3, wherein said data storage and processing means is adapted to store and process a plurality of images obtained from the image sensor in response to IR light transmitted from the IR light source through an object placed on the platen so as to determine whether the object is a live body member.

5. The apparatus of claim 4, wherein the data processing means is adapted to analyse relative intensities of said plurality of images to determine whether variations in those intensities are consistent with characteristics of a human heartbeat.

6. The apparatus of any one of claims 3 to 5 when dependent on claim 2, wherein the data processing means is adapted to process at least one image obtained from the image sensor in response to IR light transmitted from the or each IR light source through a live body member placed on the platen and at least one image obtained from the image sensor in response to visible light from the or each visible light source reflected from the live body member placed on the platen so as to determine the presence or absence of a spoofing device applied to the live body member.

7. The apparatus of any preceding claim, including at least two IR light sources for transmitting IR light through the body member, each of the IR light sources emitting IR light in a waveband that is distinguishable from the waveband of any other of the IR light sources.

8. The apparatus of any preceding claim, wherein the or each IR light source emits IR light in a waveband in the range 700 nm to 1100 nm.

9. The apparatus of any preceding claim, including a first IR light source that emits IR light with a wavelength of 850nm.

10. The apparatus of claim 9, including a second IR light source that emits IR light with a wavelength of 750 nm.

11. The apparatus of any preceding claim, including at least two visible light sources for reflecting visible light from the body member, each of the visible light sources emitting visible light in a waveband that is distinguishable from the waveband of any other of the visible light sources.

12. The apparatus of any preceding claim, wherein the image sensor is a CMOS image sensor.

13. A method for determining whether an object presented to a biometric sensor device is a live body member, comprising:

transmitting IR light from an IR light source through the object;
detecting IR light transmitted through the object using an optical image sensor;
obtaining a plurality of images from the image sensor in response to IR light transmitted from the IR light source through the object; and
processing said images to determine whether the object possesses predetermined characteristics of a live body member.

14. The method of claim 13, wherein the step of processing said images comprises analysing relative intensities of said plurality of images to determine whether variations in those intensities are consistent with characteristics of a human heartbeat.

15. A method of determining whether a live body member presented to a biometric sensor device has a spoofing device applied thereto, comprising:

transmitting IR light from at least one IR light source through the body member;
detecting IR light transmitted through the body member using an optical image sensor;
obtaining at least one image from the image sensor in response to IR light transmitted from the IR light source through the body member;
reflecting visible light from at least one visible light source from the body member;
detecting visible light reflected from the body member using the optical image sensor;
obtaining at least one image from the image sensor in response to visible light from the visible light source reflected from the body member; and
processing said images so as to determine the presence or absence of a spoofing device applied to the body member.

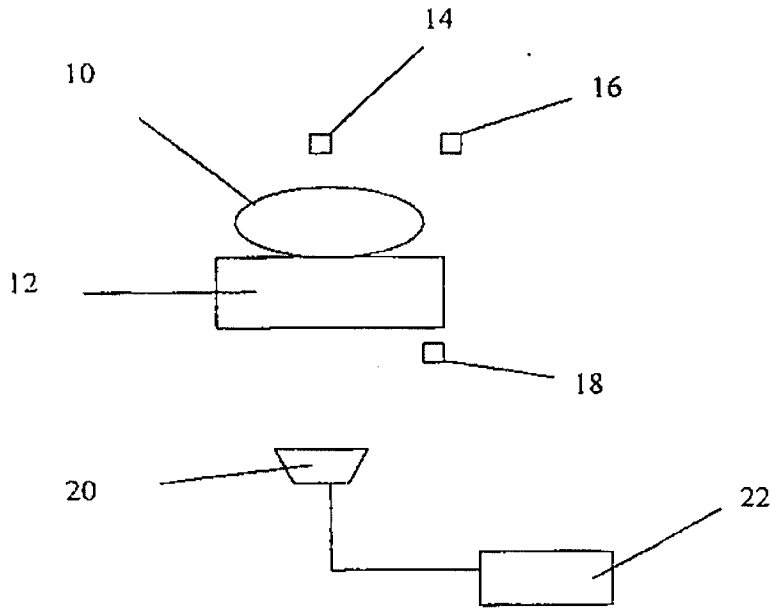

Fig. 1